



Certification Report

EAL 2 Evaluation of Xerox WorkCentre™ 7525/7530/7535/7545/7556

Issued by:

Communications Security Establishment Canada

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

© Government of Canada, Communications Security Establishment Canada, 2012

Document number: 383-4-201-CR
Version: 1.0
Date: 13 February 2012
Pagination: i to iii, 1 to 10



DISCLAIMER

The Information Technology (IT) product identified in this certification report, and its associated certificate, has been evaluated at an approved evaluation facility – established under the Canadian Common Criteria Evaluation and Certification Scheme (CCS) – using the *Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 3*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 3*. This certification report, and its associated certificate, apply only to the identified version and release of the product in its evaluated configuration. The evaluation has been conducted in accordance with the provisions of the CCS, and the conclusions of the evaluation facility in the evaluation report are consistent with the evidence adduced. This report, and its associated certificate, are not an endorsement of the IT product by the Communications Security Establishment Canada, or any other organization that recognizes or gives effect to this report, and its associated certificate, and no warranty for the IT product by the Communications Security Establishment Canada, or any other organization that recognizes or gives effect to this report, and its associated certificate, is either expressed or implied.

FOREWORD

The Canadian Common Criteria Evaluation and Certification Scheme (CCS) provides a third-party evaluation service for determining the trustworthiness of Information Technology (IT) security products. Evaluations are performed by a commercial Common Criteria Evaluation Facility (CCEF) under the oversight of the CCS Certification Body, which is managed by the Communications Security Establishment Canada.

A CCEF is a commercial facility that has been approved by the CCS Certification Body to perform Common Criteria evaluations; a significant requirement for such approval is accreditation to the requirements of *ISO/IEC 17025:2005, the General Requirements for the Competence of Testing and Calibration Laboratories*. Accreditation is performed under the Program for the Accreditation of Laboratories - Canada (PALCAN), administered by the Standards Council of Canada.

The CCEF that carried out this evaluation is CSC, Security Testing and Certification Laboratories, located in Ottawa, Canada.

By awarding a Common Criteria certificate, the CCS Certification Body asserts that the product complies with the security requirements specified in the associated security target. A security target is a requirements specification document that defines the scope of the evaluation activities. The consumer of certified IT products should review the security target, in addition to this certification report, in order to gain an understanding of any assumptions made during the evaluation, the IT product's intended environment, its security requirements, and the level of confidence (i.e., the evaluation assurance level) that the product satisfies the security requirements.

This certification report is associated with the certificate of product evaluation dated 13 February 2012, and the security target identified in Section 4 of this report.

The certification report, certificate of product evaluation and security target are posted on the CCS Certified Products list (CPL) and the Common Criteria portal (the official website of the Common Criteria Project).

This certification report makes reference to the following registered trademark:

- WorkCentre is a registered trademark of Xerox Corporation.

Reproduction of this report is authorized provided the report is reproduced in its entirety.

TABLE OF CONTENTS

Disclaimer	i
Foreword.....	ii
Executive Summary	1
1 Identification of Target of Evaluation	3
2 TOE Description	3
3 Evaluated Security Functionality	3
4 Security Target.....	3
5 Common Criteria Conformance.....	4
6 Security Policy.....	4
7 Assumptions and Clarification of Scope.....	4
7.1 SECURE USAGE ASSUMPTIONS.....	4
7.2 ENVIRONMENTAL ASSUMPTIONS	5
7.3 CLARIFICATION OF SCOPE.....	5
8 Evaluated Configuration	5
9 Documentation	6
10 Evaluation Analysis Activities	6
11 ITS Product Testing.....	7
11.1 ASSESSMENT OF DEVELOPER TESTS	8
11.2 INDEPENDENT FUNCTIONAL TESTING	8
11.3 INDEPENDENT PENETRATION TESTING.....	8
11.4 CONDUCT OF TESTING	8
11.5 TESTING RESULTS.....	9
12 Results of the Evaluation.....	9
13 Acronyms, Abbreviations and Initializations.....	9
14 References.....	9

Executive Summary

Xerox WorkCentre™ 7525/7530/7535/7545/7556 (hereafter referred to as Xerox WorkCentre™), from Xerox Corporation, is the Target of Evaluation for this Evaluation Assurance Level (EAL) 2 augmented evaluation.

Xerox WorkCentre™ is a family of multi-function devices that include copy, print, scan, and FAX functionality. The product incorporates security features such that temporary files created for these processes are encrypted and then overwritten as the processes complete. Users are required to provide a valid username and password or Common Access Card and PIN to access the product processes.

CSC, Security Testing and Certification Laboratories, is the CCEF that conducted the evaluation. This evaluation was completed on 13 February 2012 and was carried out in accordance with the rules of the Canadian Common Criteria Evaluation and Certification Scheme (CCS).

The scope of the evaluation is defined by the security target, which identifies assumptions made during the evaluation, the intended environment for Xerox WorkCentre™, the security requirements, and the level of confidence (evaluation assurance level) at which the product is intended to satisfy the security requirements. Consumers are advised to verify that their operating environment is consistent with that specified in the security target, and to give due consideration to the comments, observations and recommendations in this certification report.

The results documented in the Evaluation Technical Report (ETR)¹ for this product provide sufficient evidence that it meets the EAL 2 *augmented* assurance requirements for the evaluated security functionality. The evaluation was conducted using the *Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 3*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 3*. The following augmentation is claimed: ALC_FLR.3 – Systematic Flaw Remediation.

Xerox WorkCentre™ is conformant with the *IEEE Standard Protection Profile for Hardcopy Devices in IEEE Std 2600™ -2008 Operational Environment B (IEEE Std. 2600.2-2009)* dated 26 February 2010.

Communications Security Establishment Canada, as the CCS Certification Body, declares that Xerox WorkCentre™ evaluation meets all the conditions of the *Arrangement on the Recognition of Common Criteria Certificates* and that the product will be listed on the CCS

¹ The ETR is a CCS document that contains information proprietary to the developer and/or the evaluator, and is not releasable for public review.

Certified Products list (CPL) and the Common Criteria portal (the official website of the Common Criteria Project).

1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 2 augmented evaluation is Xerox WorkCentre™ 7525/7530/7535/7545/7556 (hereafter referred to as Xerox WorkCentre™), from Xerox Corporation.

2 TOE Description

Xerox WorkCentre™ is a family of multi-function devices that include copy, print, scan, and FAX functionality. The product incorporates security features such that temporary files created for these processes are encrypted and then overwritten as the processes complete. Users are required to provide a valid username and password or Common Access Card and PIN to access the product processes.

A detailed description of the Xerox WorkCentre™ architecture is found in Section 1.3 of the Security Target (ST).

3 Evaluated Security Functionality

The complete list of evaluated security functionality for Xerox WorkCentre™ is identified in Section 6 of the ST.

The following Government of Canada approved cryptographic algorithms were evaluated for correct implementation in Xerox WorkCentre™:

Cryptographic Algorithm	Standard	Certificate #
Triple-DES (3DES)	FIPS 46-3	826 and 1174
Advanced Encryption Standard (AES)	FIPS 197	1131 and 1821
Rivest Shamir Adleman (RSA)	FIPS 186-3	914
Secure Hash Algorithm (SHA-1)	FIPS 180-3	1599
Keyed-Hash Message Authentication Code (HMAC)	FIPS 198	644 and 1076

4 Security Target

The ST associated with this Certification Report is identified by the following nomenclature:

Title: Xerox WorkCentre™ 7525/7530/7535/7545/7556 Security Target

Version: 1.0, Revision 1.4

Date: 7 December 2011

5 Common Criteria Conformance

The evaluation was conducted using the *Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 3*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 3*.

Xerox WorkCentre™ is:

- a. *Common Criteria Part 2 extended*; with functional requirements based upon functional components in Part 2, except for the following explicitly stated requirement defined in the ST: FPT_FDI_EXP.1 - Restricted forwarding of data to external interfaces.
- b. *Common Criteria Part 3 conformant*, with security assurance requirements based only upon assurance components in Part 3; and
- c. *Common Criteria EAL 2 augmented*, containing all security assurance requirements in the EAL 2 package, as well as the following: ALC_FLR.3 – Systematic Flaw Remediation.
- d. Xerox WorkCentre™ is conformant with the *IEEE Standard Protection Profile for Hardcopy Devices in IEEE Std 2600™-2008 Operational Environment B (IEEE Std. 2600.2-2009)* Protection Profile dated 26 February 2010.

6 Security Policy

Xerox WorkCentre™ implements an IP Filtering policy, a User Access Control policy, and a TOE Function Access Control policy. In addition, Xerox WorkCentre™ implements policies pertaining to security audit, cryptographic support, identification and authentication, security management, and protection of the TSF. Further details of these security policies can be found in Section 6 of the ST.

7 Assumptions and Clarification of Scope

Consumers of Xerox WorkCentre™ should consider assumptions about usage and environmental settings as requirements for the product's installation and its operating environment. This will ensure the proper and secure operation of the TOE.

7.1 Secure Usage Assumptions

The following Secure Usage Assumptions are listed in the ST:

- TOE Users are aware of the security policies and procedures of their organization, and are trained and competent to follow those policies and procedures;
- Administrators are aware of the security policies and procedures of their organization, are trained and competent to follow the manufacturer's guidance and documentation, and correctly configure and operate the TOE in accordance with those policies and procedures; and

- Administrators do not use their privileged access rights for malicious purposes.

7.2 Environmental Assumptions

The following Environmental Assumption is listed in the ST:

- The TOE is located in a restricted or monitored environment that provides protection from unmanaged access to the physical components and data interfaces of the TOE.

7.3 Clarification of Scope

Xerox WorkCentre™ incorporates CAVP-validated cryptography and was not subjected to CMVP (FIPS-140) validation.

8 Evaluated Configuration

The evaluated configuration for Xerox WorkCentre™ comprises:

Software/Firmware Item	WorkCentre 7525/7530/7535/7545/7556
System Software	061.121.221.28308
Network Controller Software	061.121.25025
User Interface Software	061.121.24120
Marking Engine Software (Options)	
- WC 7525/7530/7535	081.077.000
- WC 7545/7556	082.077.000
Copy Controller Software	061.121.24121
Document Feeder Software (DADH)	007.008.050
Finisher Software (Options)	
- A – Finisher	013.000.000
- C – Finisher	032.042.000
- SB – Finisher	005.009.000
Fax Software	003.010.004

Software/Firmware Item	WorkCentre 7525/7530/7535/7545/7556
Scanner Software	030.141.115

The publication entitled *Secure Installation and Operation of Your WorkCentre™ 7525/7530/7535/7545/7556* describes the procedures necessary to install and operate Xerox WorkCentre™ in its evaluated configuration.

9 Documentation

The Xerox Corporation documents provided to the consumer are as follows:

- a. Xerox® WorkCentre® 7500 Series System Administrator Guide;
- b. Xerox® WorkCentre® 7500 Series User Guide;
- c. Xerox® WorkCentre® 7500 Series Quick Use Guide;
- d. Xerox® WorkCentre® 7755/7765/7775, Xerox® WorkCentre® 7500 Series, Xerox® ColorQube® 9301/9302/9303 Security-Related Supplement to User Guidance;
- e. Secure Installation and Operation of Your WorkCentre™ 7525/7530/7535/7545/7556;
- f. Xerox® WorkCentre® 7500 Series Quick Copying Guide;
- g. Xerox® WorkCentre® 7500 Series Quick Email Guide;
- h. Xerox® WorkCentre® 7500 Series Quick Faxing Guide; and
- i. Xerox® Smart Card Xerox® WorkCentre™ 7525/7530/7535/7545/7556

10 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of Xerox WorkCentre™, including the following areas:

Development: The evaluators analyzed the Xerox WorkCentre™ functional specification and design documentation; they determined that the design completely and accurately describes the TOE security functionality (TSF) interfaces, the TSF subsystems and how the TSF implements the security functional requirements (SFRs). The evaluators analyzed the Xerox WorkCentre™ security architectural description and determined that the initialization process is secure, that the security functions are protected against tamper and bypass, and that security domains are maintained. The evaluators also independently verified that the correspondence mappings between the design documents are correct.

Guidance Documents: The evaluators examined the Xerox WorkCentre™ preparative user guidance and operational user guidance and determined that it sufficiently and unambiguously describes how to securely transform the TOE into its evaluated configuration and how to use and administer the product. The evaluators examined and tested the preparative and operational guidance, and determined that they are complete and sufficiently detailed to result in a secure configuration.

Life-cycle support: An analysis of the Xerox WorkCentre™ configuration management system and associated documentation was performed. The evaluators found that the Xerox WorkCentre™ configuration items were clearly marked. The developer's configuration management system was observed during a site visit, and it was found to be mature and well-developed.

The evaluators examined the delivery documentation and determined that it described all of the procedures required to maintain the integrity of Xerox WorkCentre™ during distribution to the consumer.

The evaluators reviewed the flaw remediation procedures used by Xerox Corporation for Xerox WorkCentre™. During a site visit, the evaluators also examined the evidence generated by adherence to the procedures. The evaluators concluded that the procedures are adequate to track and correct security flaws, and distribute the flaw information and corrections to consumers of the product.

Vulnerability assessment: The evaluators conducted an independent vulnerability analysis of Xerox WorkCentre™. Additionally, the evaluators conducted a search of public domain vulnerability databases to identify Xerox WorkCentre™ potential vulnerabilities. The evaluators identified potential vulnerabilities for testing applicable to the Xerox WorkCentre™ in its operational environment.

All these evaluation activities resulted in **PASS** verdicts.

11 ITS Product Testing

Testing at EAL 2 consists of the following three steps: assessing developer tests, performing independent functional tests, and performing penetration tests.

11.1 Assessment of Developer Tests

The evaluators verified that the developer has met their testing responsibilities by examining their test evidence, and reviewing their test results, as documented in the ETR².

² The ETR is a CCS document that contains information proprietary to the developer and/or the evaluator, and is not releasable for public review.

The evaluators analyzed the developer's test coverage analysis and found it to be complete and accurate. The correspondence between the tests identified in the developer's test documentation and the functional specification was complete.

11.2 Independent Functional Testing

During this evaluation, the evaluator developed independent functional tests by examining design and guidance documentation, examining the developer's test documentation, executing a sample of the developer's test cases, and creating test cases that augmented the developer tests.

All testing was planned and documented to a sufficient level of detail to allow repeatability of the testing procedures and results. Resulting from this test coverage approach is the following list of CSC, Security Testing and Certification Laboratories, test goals:

- a. Repeat of Developer's Tests: The objective of this test goal is to repeat a subset of the developer's tests; and
- b. Independent Tests: The evaluators carried out 48 tests against the TOE claimed security functions which are identified in Section 1.3.2 of the ST.

11.3 Independent Penetration Testing

Subsequent to the independent review of public domain vulnerability databases and all evaluation deliverables, limited independent evaluator penetration testing was conducted. The penetration tests focused on:

- a. Potential network, platform and application layer vulnerabilities using automated vulnerability tools.

The independent penetration testing did not uncover any exploitable vulnerabilities in the intended operating environment.

11.4 Conduct of Testing

Xerox WorkCentre™ was subjected to a comprehensive suite of formally documented, independent functional and penetration tests. The testing took place at the Information Technology Security Evaluation and Test (ITSET) Facility at CSC, Security Testing and Certification Laboratories. The CCS Certification Body witnessed a portion of the independent testing. The detailed testing activities, including configurations, procedures, test cases, expected results and observed results are documented in a separate Test Results document.

11.5 Testing Results

The developer's tests and the independent functional tests yielded the expected results, giving assurance that Xerox WorkCentre™ behaves as specified in its ST and functional specification.

12 Results of the Evaluation

This evaluation has provided the basis for an EAL 2+ level of assurance. The overall verdict for the evaluation is **PASS**. These results are supported by evidence in the ETR.

13 Acronyms, Abbreviations and Initializations

<u>Acronym/Abbreviation/ Initialization</u>	<u>Description</u>
CCEF	Common Criteria Evaluation Facility
CCS	Canadian Common Criteria Evaluation and Certification Scheme
CM	Configuration Management
CPL	Certified Products list
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
IT	Information Technology
ITSET	Information Technology Security Evaluation and Testing
PALCAN	Program for the Accreditation of Laboratories - Canada
SFR	Security functional requirements
ST	Security Target
TOE	Target of Evaluation
TSF	TOE security functionality

14 References

This section lists all documentation used as source material for this report:

- a. CCS Publication #4, Technical Oversight, Version 1.8, October 2010.
- b. Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 3, July 2009.

- c. Common Methodology for Information Technology Security Evaluation, CEM, Version 3.1 Revision 3, July 2009.
- d. IEEE Standard Protection Profile for Hardcopy Devices in IEEE Std 2600™ -2008 Operational Environment B (IEEE Std. 2600.2- 2009), February 26, 2010.
- e. Xerox WorkCentre™ 7525/7530/7535/7545/7556 Security Target, Version 1.0, Revision 1.4, December 7, 2011.
- f. Evaluation Technical Report, Xerox WorkCentre™ 7525/7530/7535/7545/7556, Version 1.5, January 23, 2012.